AMENDMENTS TO THE CLAIMS

1.   (Currently Amended) A system for sharing a hierarchical document, the hierarchical document having a node, comprising:

a component that receives an indication of a privilege for the node, the privilege indicating access rights for the node and determined based on <u>access rights for</u> another node of the hierarchical document, the indication including a holder of the privilege;

a component that receives an access request to the node from a requestor; and

a component that handles the received access request, wherein the handling includes determining whether the requestor is a holder of a privilege that is appropriate for the received access request.

2.   (Original) The system of claim 1 wherein the holder of the privilege is a user.

3.   (Original) The system of claim 2 wherein the holder is an application program.

4.   (Original) The system of claim 2 wherein the holder is an operator of an application program.

5.   (Original) The system of claim 1 wherein the holder is a client computing device.

6.   (Original) The system of claim 1 wherein the system receives an indication of the holder from an operating system.

7.   (Original)   The system of claim 1 wherein the system authenticates the holder.

8.   (Original)   The system of claim 1 wherein the received access request is a mutation relating to a node.

9.   (Original)   The system of claim 8 wherein the indication of an access request indicates the node.

10.   (Original)   The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Insert.

11.   (Original)   The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Update.

12.   (Original)   The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Delete.

13.   (Original)   The system of claim 1 wherein the privilege is appropriate for the received access request when the received access request is Read and the privilege is Insert.

14.   (Original)   The system of claim 1 wherein the holder holds multiple privileges.

15.   (Original)   The system of claim 1 wherein the holder holds the privilege on descendants of the node merely by holding a privilege on the node.

16.   (Original)   The system of claim 15 wherein the privilege is Delete.

17.   (Original)   The system of claim 1 wherein the holder holds a different privilege on attributes of the node.

18.   (Original)   The system of claim 17 wherein the privilege is Insert and the different privilege is Read.

19.   (Original)   The system of claim 17 wherein the holder does not hold the privilege on descendants of the node merely by holding the privilege on the node.

20.   (Original) The system of claim 1 wherein the holder does not hold a privilege on a descendant of the node merely by owning the privilege on the node.

21.   (Original)   The system of claim 1 wherein the holder holds a different privilege on a parent of the node.

22.   (Original) The system of claim 21 wherein the holder is privileged to request a mutation relating to the parent.

23.   (Original)   The system of claim 22 wherein the mutation is to remove the node.

24.   (Original) The system of claim 1 wherein multiple holders hold the privilege.

25.   (Original)   The system of claim 1 wherein the holder of the privilege is a privilege group.

26.   (Original)   The system of claim 25 wherein the privilege group has multiple members.

27.   (Original) The system of claim 26 wherein the member is an application program.

28.   (Original) The system of claim 26 wherein the member is an operator of an application program.

29.   (Original) The system of claim 26 wherein the member is a client computing device.

30.   (Original) The system of claim 1 wherein the handling includes returning a message comprising an indication of mutations to users of the system.

31.   (Original) The system of claim 30 wherein the message includes only information for which a recipient of the message holds an appropriate privilege.

32.   (Currently Amended) A method in a distributed computing environment for sharing a hierarchical document, the hierarchical document having a node, comprising:
> receiving an indication of a privilege for the node, the privilege indicating access
>> rights for the node and determined based on <u>access rights for</u> another node
>> of the hierarchical document, the indication including a holder of the privilege;
> receiving an access request to the node from a requestor; and
> handling the received access request, wherein the handling includes determining
>> whether the requestor is a holder of an appropriate privilege for the received
>> access request.

33.   (Original) The method of claim 32 wherein the holder of the privilege is a user.

34.   (Original)   The method of claim 33 wherein the holder is an application program.

35.   (Original)   The method of claim 33 wherein the holder is an operator of an application program.

36.   (Original)   The method of claim 32 wherein the holder is a client computing device.

37.   (Original)   The method of claim 32 wherein the system receives an indication of the holder from an operating system.

38.   (Original)   The method of claim 32 wherein the system authenticates the holder.

39.   (Original)   The method of claim 32 wherein the received access request is a mutation relating to a node.

40.   (Original)   The method of claim 39 wherein the indication of an access request indicates the node.

41.   (Original)   The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Read.

42.   (Original)   The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Insert.

43.   (Original)   The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Update.

44. (Original) The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Delete.

45. (Original) The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation is Read and the privilege is Insert.

46. (Original) The method of claim 32 wherein the holder holds multiple privileges.

47. (Original) The method of claim 32 wherein the holder holds the privilege on descendants of the node merely by holding a privilege on the node.

48. (Original) The method of claim 47 wherein the privilege is Delete.

49. (Original) The method of claim 32 wherein the holder holds a different privilege on attributes of the node.

50. (Original) The method of claim 49 wherein the privilege is Insert and the different privilege is Read.

51. (Original) The method of claim 49 wherein the holder does not hold the privilege on descendants of the node merely by holding the privilege on the node.

52. (Original) The method of claim 32 wherein the holder does not hold a privilege on a descendant of the node merely by owning the privilege on the node.

53. (Original) The method of claim 32 wherein the holder holds a different privilege on a parent of the node.

54.   (Original) The method of claim 53 wherein the holder is privileged to request a mutation relating to the parent.

55.   (Original) The method of claim 54 wherein the mutation is to remove the node.

56.   (Original) The method of claim 54 wherein the mutation is to remove an attribute.

57.   (Original)   The method of claim 32 wherein multiple holders hold the privilege.

58.   (Original) The method of claim 32 wherein the holder of the privilege is a privilege group.

59.   (Original) The method of claim 58 wherein the privilege group has multiple members.

60.   (Original) The method of claim 59 wherein the member is an application program.

61.   (Original) The method of claim 59 wherein the member is an operator of an application program.

62.   (Original) The method of claim 59 wherein the member is a client computing device.

63.   (Original) The method of claim 32 wherein the handling includes returning a message comprising an indication of mutations to users of the system.

64.   (Original)   The method of claim 63 wherein the message includes only information for which a recipient of the message holds an appropriate privilege.

65.   (Original)   The method of claim 32 wherein the access request identifies the node with a unique identification.

66.   (Original)   The method of claim 32 wherein the access request is received as a message.

67.   (Original)   The method of claim 66 wherein the message is represented in XML.